IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	**Case No. 1:16CR228**
	)	
RUSLANS BONDARS	)	
	)	
Defendant.	)	

DEFENDANT'S POSITION ON SENTENCING

A sentence of 18 months incarceration is sufficient, but not greater than necessary, to comply with the purposes enunciated by Congress in 18 U.S.C. § 3553(a)(2).

Mr. Bondars elected to proceed to trial in this case on advice of counsel. In doing so, the Court should not perceive Mr. Bondars to be obstinate or exempt from responsibility. For at trial, Mr. Bondars did not assert a fantastical defense such as arguing he was not the administrator of Scan4You, or didn't use the seized computer devices. In fact, he didn't even maintain that he was unaware of the customer base to which Juri Martisevs advertised the service. He did not deny that he and Juri had engaged in questionable behavior in the past.

Instead, through counsel, Mr. Bondars took full ownership of his conduct. He acknowledged that he created and administered Scan4You with the awareness of the forums through which it was advertised. Mr. Bondars' trial was simply about arguing the

legal insufficiency of the conduct to the charged offenses and maintaining the ability to challenge the government's outrageous loss amounts.[1]

For these reasons, Mr. Bondars' should receive acceptance of responsibility. However, at the very least, he should not be punished more harshly than those who pled guilty. *See* U.S.G. § 3E1.1 App. Note 2; *United States v. Shires*, No. 98-4635, 1999 U.S. App. LEXIS 9027 (4th Cir. May 10, 1999); *United States v. Schultz*, 917 F. Supp. 1343, 1351 (N.D. Iowa 1996) ("Both the application notes to § 3E1.1 and case law further develop the distinction between *factual* disputes over guilt, which indicate a failure by the defendant to recognize and accept responsibility for his or her conduct, and *legal* disputes over guilt.") (emphasis in original).

Additionally, in contemplating Mr. Bondars' request for an 18-month sentence, counsel did not pluck an abstract number from thin air. Mr. Bondars' request is a product of carefully considered factors, including the nature of his conduct and the sentences of the more culpable defendants in his case. Specifically, on the following points:

- The defendants who testified against Mr. Bondars, (Shames, Vartanyan, and Belorossov) and one who didn't testify, Taylor Huddleston, all *developed* and *deployed* malware, essentially stealing people's information for a living.

- These individuals earned more money and created a more potent product that could only be used for criminal purposes.

[1] The PSR responds that Martisevs pled guilty and still "reserved the right to argue the appropriate loss amount at sentencing." PSR p. 25. Mr. Bondars does not perceive this to be accurate from a practical perspective. Though Martisevs' Plea Agreement did not prescribe a loss amount via Rule 11 (c)(1)(B) guidelines, the PSR fails to consider that Martisevs' Statement of Facts essentially concedes the loss amount by stating that he was involved in 2013 "Computer Intrusions Against Major U.S. Retailer." ECF No. 71 at 9. Therefore, the idea that Martisevs' plea agreement allowed him to challenge the government's application of this speculative loss amount is a legal fiction when assessed with the accompanying Statement of Facts. A true plead-and-argue scenario would not include a defendant's concession to the very facts the government needs to prove on loss.

- Scan4You was a small fraction of all the components that went in to developing and deploying malware and had potential legitimate uses. Thus, all three malware developers and users who testified against Mr. Bondars are substantially more culpable than Mr. Bondars.

- These more culpable individuals pled guilty and received sentences of six months, (Shames) 48 months (Huddleston), 54 months, (Belorossov) and 60 months (Vartanyan). Two of these sentences included cooperation reductions.

- ReFUD.me, the individual in the United Kingdom that the Government repeatedly referenced during trial as offering a similar scanning service also sold his own malware. Therefore, he was more culpable than Mr. Bondars. He received a sentence of two years. *See* Gareth Corfeild, *Essex black hat behind Cryptex and reFUD gets two years behind bars*, The Register (Feb 15, 2018).[2]

- Finally, even if the Court determines a trial penalty is warranted, it should not amount to decades, or even years, more than these other more culpable defendants. A trial penalty of this magnitude would undermine the Sixth Amendment right to trial to the point it becomes meaningless.

GUIDELINES OBJECTIONS

Pursuant to Rule 32 of the Federal Rules of Criminal Procedure, and Section 6A1.3 of the advisory United States Sentencing Guidelines, the Defendant, Ruslans Bondars, by counsel, states that he has received and reviewed the Presentence Investigation Report ("PSR"). Mr. Bondars has eight factual corrections or clarifications, and four Guidelines objections. Specifically, Mr. Bondars objects to the loss amount, the leadership enhancement, the intent to obtain personal information enhancement, and argues he should receive acceptance of responsibility.

A. Factual Objections

¶¶13-39 – Mr. Bondars makes a general objection to the entire characterization of the offense conduct.

[2] Available at https://www.theregister.co.uk/2018/02/15/refud_cryptex_kingpin_goncalo_esteves_jailed/ (last accessed Sept 11, 2018).

¶16 – There has been no evidence presented that scan4you was the largest service of its kind. In fact, the Court heard evidence of several other scanners widely-used within the same underground community. Additionally, the second sentence should read "scanned millions of files," omitting the word "malicious." The Government has not examined millions of files run through scan4you. In fact, the Government only examined hash values in this case, not any of the actual the files run through scan4you. Therefore, the government cannot attest millions of malicious files.

¶20 – "BONDARS" should be omitted from this paragraph because it contradicts the prior paragraph which correctly indicated that Martisevs handled the advertising.

¶21 – Mr. Bondars was unaware of scan4you franchisees. This is confirmed in the 1/22/2018 FBI 302 Report, ("MARTISEVS did not always consult with BONDARS when resellers contacted him).[3]

¶24 – Disabling automated reports to antivirus companies is a standard feature on the antivirus products. Any user can turn off the reporting if he does not want this information sent back to the antivirus company. *See* T.T. 658, 662, *Testimony of Robert McArdle*; *See* T.T. 801 *Testimony of Vikrum Thakur*.

¶27 – The second sentence of this paragraph mischaracterizes the evidence. Martisevs and Bondars did not provide this particular co-conspirator with access to scan4you. The scan4you service was a publicly-available, automated, online program that any person could sign up for to gain access. Neither Martisevs nor Bondars "provided" this person with access to the service, any more than yahoo or google "provides" email services to a user who simply registers.

Additionally, neither Martisevs nor Bondars knew that this co-conspirator would use scan4you to develop malicious software. This user never communicated with Bondars or Martisevs at all. There were legitimate users of the service, *See* T.T. 840-42, *Testimony of Kevin Peden*; T.T., 760-61 *Testimony of Juris Martisevs* (noting the emails from Nosibay company located in France, and an email from Leo Impact Security inquiring about a corporate account). Simply being a scan4you user did not mean that person was developing malicious software to be used for illegal computer intrusions.

¶32 – Objection to the characterization of the evidence for the same reasons outlined above in ¶27.

¶69 – These websites were registered using Martisevs' phone number.

[3] This report was produced to the Court accompanying Mr. Bondars' Motion to Dismiss with Prejudice filed under seal during trial.

B. Loss Amount Objection

Mr. Bondars objects to the loss amount calculated in the Guidelines for five reasons: 1) The evidence on loss amount with respect to the Citadel and Limitless logger is deficient and overstated; 2) With respect to the Target data breach, Mr. Bondars was not convicted of conspiring with or aiding and abetting user number 958; 3) Mr. Bondars' service did not assist user 958 as a purely factual matter; 4) The Target data breach is not relevant conduct because it was not within the scope of jointly undertaken criminal activity or in furtherance of that criminal activity; and 5) the loss amount was not foreseeable.

Mr. Bondars also objects to the 3B1.1(a) leadership enhancement, and the application of 2B1.1(b)(17) that attributes an intent to obtain personal information.

I. The evidence on loss amount with respect to the Citadel and Limitless logger is deficient and overstated as to Scan4You's involvement.

The Government's loss amount evidence is deficient. Unsupported assertions such as "theft of over 40 million credit card numbers," "malware caused approximately $3,369,400," and "industry estimates," with nothing more, are not sufficient evidence of loss amount. PSR ¶41, 42, 43. The Government provided no actual evidence of this loss.

Furthermore, the Citadel and Limitless Logger only incorporated scan4you for a small period of time within its lifecycle. Therefore, the loss would need to be calculated exclusively within those time-frames. *See* T.T. 140-41, *Testimony of Zachary Shames*; T.T. 221-22, *Testimony of Mark Vartanyan*. Testimony of the Limitless Logger developer and the Citadel support developer indicated that they did not know if the user of their malware actually used Scan4You. These individuals distributed a toolkit, but had no idea which tools were used from that kit, and did not personally use their own malware.

Therefore, simply because scan4you was incorporated into the malware toolkit not mean that any of the users of chose to use it to cause any loss.

Finally, Belorossov, a Citadel user who actually stole personal information on the internet, originally said he used a different scanner. *See* T.T. 255. Belorossov himself did not commit all of the Citadel computer intrusions, and at sentencing he was only held responsible for a fraction of the total number of intrusions caused by the Citadel. No one knows whether other Citadel users used scan4you. It is also unclear for how many of Belorossov's computer intrusions he used scan4you, over what period of time, and what, if any, measure of losses it caused.

II. Mr. Bondars was not convicted of conspiring with or aiding and abetting user number 958

Unlike Mr. Martisevs, Mr. Bondars did not sign a Statement of Facts that implicates him in a November 2013 retail data breach. *See* ECF No. 71 at 9. That is because he did not know of such data breach, and never conspired to commit, or aided and abetted, such a data breach. Moreover, the jury in this case did not convict him of this conduct.

Trial testimony consisted of four alleged co-conspirators, Juri Martisevs, Zachary Shames, Dimitri Belorrosov, and Mark Vartanyan. The Government also elicited testimony about a "user 958," (on the Target databreach). *See* T.T. 592-95. During deliberations, the jury asked several questions that illuminated who the jury contemplated as Mr. Bondars' co-conspirator, and what conduct it contemplated Mr. Bondars aided and abetted.

The jury first asked if it could consider evidence outside the time periods listed in the superseding indictment. *See* T.T. 1001. In essence, the jury asked if it could consider the 404(b) chat messages between Ruslans and Jurijs that described other bad acts, as

substantive evidence. Second, the jury asked if a defendant could aid and abet someone he was already in a conspiracy with, and then requested to see the transcript of the co-defendant, Juris Martisevs,' testimony in the same question. *See* T.T. 1009-10. There were no questions that requested information about any other alleged co-conspirator.

In total, the jury asked six questions, none of which indicated they were contemplating convicting Mr. Bondars of the 2013 retail data breach. Furthermore, the jury acquitted Mr. Bondars of aiding and abetting the substantive wire fraud offense, showing once again, that it did not believe the evidence stretched so far as to actually convict him of this type of crime. If the jury considered User 958 to be a co-conspirator in the Target data breach, the jury would have convicted Mr. Bondars of wire fraud.

III. Mr. Bondars did not assist in the Target data breach as a purely factual matter.

The evidence showed that, while user 958 used Scan4You, that service, and especially Mr. Bondars himself, did not assist in the Target data breach. First, the hash values found on the Target server were actually flagged by many of the anti-virus companies when run through Scan4You, and by Target's own antivirus software. *See* T.T. 282-84 Testimony of Daniel Ryan ("Q: …[T]here were two occasions where their security software picks something up? A: Yes. Q: Then they just didn't know what it was or didn't know where to look, and it kind of went under the radar? A: It seems that way."). Moreover, as each file was scanned, it actually became more detectable, (or stayed the same) not less detectable in the system. *See* T.T. 600-02, *Testimony of Agent Kim*. Thus, the argument that Scan4You helped user 958 ensure the undetectability of his file, is belied by the evidence. It *was* detected, both in the Scan4You database, and in Target's system.

Second, these same hash values used in the Target data breach were actually run through Virus Total – the Google-owned and "legitimate" file scanning service, according to the Government – around the same time. *See* T.T. 823-24, *Testimony of Heather Shannon*. This means any argument that Scan4You assisted because of its anonymity feature, is also undercut because this user obviously was not concerned about anonymity.

Third, the person or persons who committed the Target data breach had already been inside the Target network for about one week prior to the breach, and "none of the these five files [listed in the Scan4You database] actually got them into the network." *See* T.T. 278-79, *Testimony of Daniel Ryan*.

Therefore, for all of these reasons, as a simple matter of fact, Mr. Bondars did not aid and abet the Target data breach (knowing that the crime was being committed or about to be committed) and Mr. Bondars did not conspire with user 958 to commit the Target data breach.

IV. The Target data breach is not relevant conduct because it was not within the scope of jointly undertaken criminal activity or in furtherance of that criminal activity.

Losses from the Target data breach, Citadel, and Limitless Logger cannot be considered relevant conduct because they were not "within the scope of the jointly undertaken criminal activity," or "in furtherance of that criminal activity" under §1B1.3(a)(1)(B)(i). "For two or more offenses to constitute part of a common scheme or plan, they must be substantially connected to each other by at least one common factor, such as common victims, common accomplices, common purpose, or similar modus operandi." *See id*.

The jointly undertaken activity is referred to as "the scope of the specific conduct and objectives embraced by the defendant's agreement." Application Note 3(B). More importantly, "Acts of others that were not within the scope of the defendant's agreement, even if those acts were known or reasonably foreseeable to the defendant, are not relevant conduct under subsection (a)(1)(B)." Id. (emphasis added).

Further, Application Note 4(C)(i) of §1B1.3 provides an example similar to Mr. Bondars' situation:

> (i) Defendant D pays Defendant E a small amount to forge an endorsement on an $ 800 stolen government check. Unknown to Defendant E, Defendant D then uses that check as a down payment in a scheme to fraudulently obtain $ 15,000 worth of merchandise. Defendant E is convicted of forging the $ 800 check and is accountable for the forgery of this check under subsection (a)(1)(A). Defendant E is not accountable for the $ 15,000 because the fraudulent scheme to obtain $ 15,000 was not within the scope of the jointly undertaken criminal activity (i.e., the forgery of the $ 800 check).

Just as in this example, Mr. Bondars' conduct in developing Scan4You, a publicly-available automated service where users can scan files, is separate and distinct from User 958's fraud scheme, the Citadel user's fraud, and the Limitless Logger's fraud (whose actual perpetrators are unknown). This was not a "common scheme or plan," or jointly undertaken criminal activity. See §1B1.3 Application Note 5(B)(i). Mr. Bondars created a publicly available, online, automated computer program that allowed a user – any member of the public – to scan files. He had no knowledge of – or interest in – specific users' subsequent fraud schemes, and they were at least two degrees removed from Mr. Bondars.

The malware developer created malware, who then sold that malware toolkit to a user who may have used it to commit fraud. Direct testimony from the developers provided no evidence on what percentage, if any, of the users actually used Scan4You.

Furthermore, Mr. Bondars did not stand to benefit in any respect from any user's fraud scheme of which he was unware. The conduct of these second and third degree users were not "the scope of the specific conduct and objectives embraced by the defendant's agreement." Application Note 3(B). Therefore Mr. Bondars' conduct was not "jointly undertaken criminal activity," or an action to further that criminal activity. See §1B1.3(a)(1)(B).

The jury's questions that focused on Martisevs, and the evidence, showed that Mr. Bondars never formed an agreement with the users of his service because he set up the service, and it simply ran automatically. Even if he had any relationship with users at all, it not to commit the crimes of these specific frauds. The Court acknowledged this about this case as well:

> The Government made no allegation that Defendant had specific knowledge of particular computer intrusions, but rather advanced a theory of the case that emphasized Defendant's broad knowledge of his services' functional application.

United States v. Ruslans Bondars, 1:16CR228, Order on Motion to Dismiss, ECF No. 197.

V. This unsubstantiated loss amount was not foreseeable

The U.S. Sentencing Guidelines Manual states that when a defendant's enumerated offenses are subject to enhancement based on loss amount, the actual loss is defined as the reasonably foreseeable pecuniary harm that resulted from the offense. U.S. Sentencing Guidelines Manual § 2B1.1 cmt., application n. 3(A). The Guidelines further clarify that reasonably foreseeable pecuniary harm is harm that the defendant knew, or under the circumstances, reasonably should have known, was a potential result of the offense. U.S. Sentencing Guidelines Manual § 2B1.1 cmt., application n. 3(A)(iv) and

3(D)(i). “A defendant charged with participating in a conspiracy only can be held accountable for the reasonably foreseeable acts of others that are taken in pursuit of the criminal activity she agreed to join.” *United States v. Gilliam*, 987 F.2d 1009, 1012-14 (4th Cir. 1993).

Due to the complex and often difficult nature of determining foreseeability, the courts have not created a bright-line test for assessing whether loss amounts were reasonably foreseeable to a defendant. Rather, courts apply what is functionally a “totality of the evidence” standard, referred to as a “relevant conduct” examination. The courts weigh the relevant conduct of the defendant to determine whether the loss amount of the total conspiracy was reasonably foreseeable to each of the individuals within the conspiracy. *United States v. Bolden*, 325 F.3d 471, 498 (4th Cir. 2003). One participant in a multi-participant conspiracy may be held accountable, for sentencing purposes, for a greater or lesser amount than co-participants. *United States v. Gilliam*, 987 F.2d 1009, 1013 (4th Cir. 1993). Courts have suggested that among the factors to be considered for determining foreseeability are similarities in modus operandi, knowledge of the scope of the scheme, and length and degree of defendant’s participation. *United States v. Duncan*, 2013 U.S. Dist. LEXIS 129629 (citing 657 F.3d 560, 564 (7th Cir. 2011) and § 1B1.3 of the United States Sentencing Commission).

Courts in the 4th Circuit have often held that a loss amount may only be attributed to a defendant where he played some substantive role in causing the loss. Defendants whose roles were far more involved in a conspiracy than Mr. Bondars’ have been found unable to foresee the loss amount leveled against them. In *United States v. Jinwright*, a husband and wife conspired to defraud the United States through tax fraud. 683 F.3d 471

(4th Cir. 2012). Mr. & Mrs. Jinwright hid the taxable income they received from working at their church as a pastor and committee member, respectively. Ms. Jinwright was aware that her husband was falsifying their joint tax returns from 1991 to 1993 and she directly benefitted from that fraud. However, the court found the loss amount of the tax fraud was only foreseeable to Ms. Jinwright in 1998, when she began engaging in the identical practices to her husband to hide their fraudulent activity. Despite the fact that she had been explicitly aware of the fraud being committed by her husband on behalf of both of them and had benefitted from that fraud for years, the court ruled that her knowledge of her husband's wrongdoing was not enough for her to reasonably foresee that the loss amount may also be levelled against her for sentencing purposes.

All of the factors listed in *Duncan* and the Guidelines – similarities in *modus operandi*, knowledge of the scope of the scheme, and length and degree of defendant's participation – all direct a finding that the government's loss amount was not foreseeable. The loss amount in the PSR is derived from *four users out of 31,916 users*, and *five files out of over 14 million jobs* run through this program. Mr. Bondars was not familiar with these users, had no interaction with them, and did not know, or share, their *modus operandi* or the scopes of their individual scheme. Not only was Mr. Bondars' role limited to technical administrator for an automated online website, it would have been impossible for him to examine every file of the millions scanned through the program, or have an understanding of every user's intent – whether nefarious or legitimate.

It is unreasonable to believe that Mr. Bondars should have anticipated, in any measurable capacity, the enormous loss amount that came as a result of four users of 31,916 users and five files out of over 14 million jobs run through the service.

Furthermore, the Government cannot argue that Mr. Bondars should have anticipated this potential loss amount because his service was advertised to "hackers" generally. That would mean that any anyone involved in a computer intrusion case, or anyone who has "hackers" use their service, would automatically have billions of dollars in loss applied to their sentencing calculation because that is always a potential result of engaging with "hackers." Not only does case-law dictate that there must be something more than simply this broad and general assertion, Agent Kim himself testified that he only investigated six out of approximately 31,000 users. *See* T.T. 589. The testimony was as follows:

Q. So out of 31,000 users, you've only reviewed four?

A. I could have reviewed maybe half -- six maybe, something like that.

Q. Out of 31,000?

A. Yes, sir.

Q. So can you testify to any of the legitimate clients that Scan4you had

A. I haven't reviewed the other clients' information.

Therefore, a general assertion that the service was advertised on hacker forums, when the Agent himself can only attest to reviewing six of the 31,000 users, is not sufficient to hold him accountable for the actions of one isolated actor – or even six isolated actors – when the rest of the 31,000 users could be completely legitimate. To say that Mr. Bondars should have foreseen the actions and loss from these isolated users with whom he never communicated, had no knowledge of, who was one of 31,000 users, and scanned five files out of millions is inconsistent with the case-law, the Guidelines manual, and common sense.

The government's argument that accuses the defendant of taking position that creates a "create a perverse incentive for criminals to operate websites with absurdly large criminal followings, just to thwart criminal prosecution" is misplaced. *See* ECF No. 198 at 9. In fact, defendant's position is critical to protecting millions of legitimate online services, whereas the Government's overly-broad theory places almost all online businesses in jeopardy.

Contrary to the Government's assertion, the inquiry does not begin with examining the total volume of customers. First, a distinction must be made between website that operate exclusively for criminal purposes versus those that have both legitimate and illegitimate aims. This distinction is critical to determining whether the Court must find that the defendant knew of, or formed an agreement with, a customer who intended to commit a crime. For example, imagine if the operators of TOR, or gmail, yahoo, or any publicly available website were criminally responsible for actions of a single user. Certainly these businesses have hundreds of thousands, if not millions, of users who use their programs for criminal aims. Contrast this with the Limitless Logger or Citadel developers. These malware developers have customers who could *only* have criminal goals in purchasing the malware because that malware has only one purpose.

This why the initial distinction between services that deal *exclusively* in criminal affairs and those that have both legitimate and illegitimate uses is so critical. In an exclusively criminal enterprise, the Government doesn't have to know each and every actor because the *only* agreements that could be formed are illegal ones. Comparatively, in a program with both legitimate and illegitimate purposes, the defendant cannot simply be held responsible for a few isolated actors. The Government's overly broad theory –

that if a person's website is often used by unsavory characters, he is automatically responsible for every act of every customer – would create a limitless list of online websites that could find themselves the subject of criminal prosecution and absurd loss amounts.

In this case, the evidence from multiple witnesses showed Scan4You had both legitimate and illegitimate uses, *see* T.T. 817-19, *Testimony of Heather Shannon*, and legitimate and illegitimate clients. *See* T.T. 840-42, *Testimony of Kevin Peden*; T.T., 760-61 *Testimony of Jurijs Martisevs* (noting the emails from Nosibay company located in France, and an email from Leo Impact Security inquiring about a corporate account); Def.'s Ex. 2, *Def.'s Trial Exhibits G and H*. Not every customer was a criminal, which means that not every "agreement" was a criminal conspiracy. Thus, Mr. Bondars needed some type of additional information to make a $20.5 Billion loss amount foreseeable.

Instead, the loss amount in this case should be half of the earnings of Martisevs and Bondars, $62,884.935, which is half of the forfeiture amount in Martisev's plea agreement. See USSG §2B1.1 Application Note 3(B). This would be a 6-point enhancement under USSG §2B1.1(b)(1)(D).

C. Other Guidelines Objections

I. Mr. Bondars was not a leader, and instead, should receive a decrease of 4 levels for being a minimal participant.

Mr. Bondars objects to the 3B1.1(a) leadership enhancement. Rather than a leader, Mr. Bondars was a minimal participant. To apply the leadership enhancement the PSR takes a position in ¶47 that Mr. Bondars and Martisevs were the only two individuals in the conspiracy. This position is inconsistent with the prior sections of the PSR which, in order to establish $20.5 billion in loss enhancement, finds that the users of

scan4you – the malware developers and their clients – were part of the conspiracy. This would mean Mr. Bondars would have a minimal role, and the malware developers and users would be the leaders.

In fact, the government itself conceded that "Malware developers like [Shames/Huddleston] are the root cause of computer hacking." *United States v. Zachary Shames*, 1:16CR289 – LO, *Gov. Position on Sentencing*, ECF No. 30 at 2; *United States v. Taylor Huddleston*, 1:17CR34-LO, ECF No. 40 at 12. The government further acknowledged that "In the cybercrime world, malware developers are at the heart of the problem." *Shames*, ECF No. 30 at 9; *Huddleston*, ECF No. 40 at 13. The purpose, and *only* purpose of malware created by developers, like Shames, Huddleston, Vartanyan, and used by users like Belorossov, was to infiltrate a computer system and extract personal information for their own financial gain.

Contrast this behavior with Mr. Bondars' conduct. Mr. Bondars did not develop or sell malware. *See* T.T. 580, *Testimony of Agent Kim* ("Q: Did you ever find any evidence of that? A: No, I did not."). He also did not use malware himself to commit fraud. Mr. Bondars' role in what the government called the "root cause" of computer hacking, was extraordinarily tangential.

Mr. Bondars' service was a small piece of the vast array of other tools used by malware developers – tools that the Governments' own witnesses acknowledged assisted these developers in creating and distributing malware. *See* T.T. 146, *Testimony of Zachary Shames* (noting that other individuals, Mava Maarten, SomeWhiteGuy, and Aeonhack all assisted him in developing and distributing his malware); T.T. 190-195, *Testimony of Mark Ray* (noting that sendspace.com and TOR assisted malware

developer); T.T. 250-51, *Testimony of Dimitri Belorossov* (discussing that exploit.in assisted him, doublevpn.com assisted him, encrypted chat services assisted him). To illustrate this stark disparity, consider the fact that the Citadel sold for several thousand dollars, whereas the cost of scanning a file on scan4you was 15 cents per file or $25 per month. *See* T.T. 250, *Testimony of Dimitri Belorossov*; T.T. 727, *Testimony of Jurijs Martisevs.*

Not only was Scan4You a small tool, it was a relatively generic tool that was offered by others in the business as well. *See* T.T. 138-141, *Testimony of Zachary Shames* (noting that he advised his customers to use other scanners, and he himself used two different scanners, not Scan4You towards the end of his keylogger business); Def. Ex. A; T.T. 255, *Testimony of Dimitri Belorossov* (stating he used Virtest scanner at one point). Providing one of several generic tool options for malware developers is hardly akin to developing the actual unique potent malware itself. Mr. Bondars disputes the assertion in the PSR that scan4you "played an integral role in the success of hacker's criminal activity." PSR p. 25. As described above, these individuals used a variety of scanners, and sometimes did not use scanners at all. In the situation with User 958, scan4you was not integral at all since his file became more detectable, not less detectable as it was run through scan4you, and was in fact, detected by Target's antivirus software.

Furthermore, unlike the perpetrators of the computer intrusions and wire frauds, Mr. Bondars did not have any personal or financial interest in their crime. As the guidelines prescribe, "a defendant who does not have a proprietary interest in the criminal activity and who is simply being paid to perform certain tasks should be considered for an adjustment under this guideline." USSG §3B1.2, *Application Note* 3(C).

Examining the application note factors, the conclusion that Mr. Bondars was a minimal participate is clear.

> (i) the degree to which the defendant understood the scope and structure of the criminal activity;
>
> *Mr. Bondars had no knowledge of any specific wire fraud or computer intrusion being planned or committed by the malware developers or the malware developer's clients.*
>
> (ii) the degree to which the defendant participated in planning or organizing the criminal activity;
>
> *Mr. Bondars played no role in planning a wire fraud or computer intrusion with the users of scan4you.*
>
> (iii) the degree to which the defendant exercised decision-making authority or influenced the exercise of decision-making authority;
>
> *Mr. Bondars exercised no decision-making authority or influence on a decision for a wire fraud or computer intrusion with the users of scan4you.*
>
> (iv) the nature and extent of the defendant's participation in the commission of the criminal activity, including the acts the defendant performed and the responsibility and discretion the defendant had in performing those acts;
>
> *As explained above, Mr. Bondars role was limited to providing the technical instruction for a publicly available, automated, generic tool, that provided one out of many components of a malware toolkit to malware developers and users.*
>
> (v) the degree to which the defendant stood to benefit from the criminal activity.
>
> *Mr. Bondars had no financial, or personal, interest in the wire fraud or computer intrusion of a scan4you user.*

USSG §3B1.2, *Application Note* 3(C).

With respect to Mr. Bondar's relationship with Martisevs, Martisevs played a larger role in scan4you than Mr. Bondars. Martisevs interacted with clients, advertised and promoted the service, and developed new business ideas to grow scan4you (such as the franchising and relationship with reFUD.me), often without consulting Mr. Bondars. Mr. Bondars acted at Martisev's requests. Additionally, scan4you was Martisevs' main

(if not only) source of income, whereas Mr. Bondars had a full-time career in Information Technology for a company where he worked for a decade. Therefore, Martisevs was the driving force behind the business. In fact, the chat messages reveal that when Bondars asked Martisevs about possibly closing the business, it was clear that the decision as to whether to do so rested with Martisevs. *See* Gov. Ex. 12, p. 1; Gov. Ex. 20, p. 1-3.

Additionally, and importantly for Mr. Bondars' case, "a defendant who is accountable under §1B1.3 for a loss amount … that greatly exceeds the defendant's personal gain from a fraud offense or who had limited knowledge of the scope of the scheme may receive an adjustment under this guideline." USSG §3B1.2, *Application Note* 3(A).

II. Mr. Bondars should not receive an enhancement for intent to obtain personal information, and should also receive acceptance of responsibility.

Mr. Bondars also objects to the enhancement of 2B1.1(b)(17) that attributes an intent to obtain personal information to Mr. Bondars conduct. As discussed above, Mr. Bondars had no interest in the subsequent fraud of his customers, and did not build or operate Scan4You with that intent. There was no evidence presented that Mr. Bondars himself engaged in obtaining personal information, received personal information, or had any interest in receiving or obtaining such information. Therefore 2B1.1(b)(17) should not apply.

Finally, Mr. Bondars should receive acceptance of responsibility for the reasons described *supra* p. 1-2.

In sum, the Guidelines calculation should be as follows:

§2X1.1(a), §2B1.1, Base Offense Level	+7
USSG §2B1.1(b)(1)(D), Loss $40,000-$95,000	+6
USSG §2B1.1(b)(2)(A)(i), 10+ victims	+2
USSG §2B1.1(b)(10)(B)&(C), soph means	+2
USSG §2B1.1(b)(18)(A)(ii), offense §1030(a)(5)(A)	+4
USSG §3B1.2(a), minimal participant	-4
USSG §3E1.1, acceptance of responsibility	-2
Total offense level	15

Offense Level 15, Criminal History Category I = GL: <u>18-24 MONTHS</u>

BACKGROUND

Ruslans Bondars was born into what is now communist Russia. He and his parents fled when he was a small child, and he was raised in Riga, Latvia. His parents had little, and they stretched their small earnings to provide for Ruslans and his disabled sister. During his childhood he relied on the family of his friend and neighbor, Juri Martisevs, for companionship and financial support. He hoped one day he could repay him.

As it turns out, Ruslans could. While Juri floated from job to job, unable to settle into a career, Ruslans developed his programming skills. Eventually, Ruslans became well-known and respected in his field. He began working for a company now called Dynnino, and rose through its ranks. Ruslans had been working there almost a decade when he was arrested.

During this period, Juri reached out to Ruslans with his new and exciting ideas for

computer programing schemes. One of these ideas was Scan4You. He asked Ruslans if he would be able to build a program like Virus Total using off-the-shelf antivirus products, and turning off the reporting back feature.[4] Ruslans believed he could, and soon Scan4You was born.

Ruslans built and administered the program while Juri handled the marketing and customer support. Almost Juri's entire income was derived from Scan4You while Ruslans had a full-time career. Between the two, Juri was the individual who interacted with customers. This left Ruslan relatively insulated from knowing specific pursuits of their endeavors.

One morning as he sat in his office at work in Riga, Latvia, the FBI and Latvian Police stormed the building, arrested Mr. Bondars, and brought him to the United States to be tried for these criminal offenses.

ARGUMENT

I. Legal Standard

In *Kimbrough v. United States*, 128 S. Ct. 558 (2007), and *Gall v. United States*, 128 S. Ct. 586 (2007), the Supreme Court held that the Sentencing Guidelines are simply an advisory tool to be considered alongside other statutory considerations set forth in 18 U.S.C. § 3553(a). In two summary reversals, moreover, the Court stated unequivocally that the Guidelines cannot be used as a substitute for a sentencing court's independent determination of a just sentence based upon consideration of the statutory sentencing factors. *Nelson v. United States*, 129 S. Ct. 890 (2009); *Spears v. United States*, 129 S.

[4] Disabling the reporting back function is a feature available to any user of the product if he does not want this information sent back to the antivirus company. *See* T.T. 658, 662, *Testimony of Robert McArdle*; See T.T. 801 *Testimony of Vikrum Thakur*.

Ct. 840 (2009). "Our cases do not allow a sentencing court to presume that a sentence within the applicable Guidelines range is reasonable," the Court held in *Nelson*. 129 S. Ct. at 892. "The Guidelines are not only *not mandatory* on sentencing courts; they are also not to be *presumed* reasonable." *Id*. at *2 (emphasis in original). In other words, sentencing courts commit legal error by using a Sentencing Guidelines range as a default to be imposed.

Congress has required federal courts to impose the least amount of imprisonment necessary to accomplish the purposes of sentencing as set forth in § 3553(a) of Title 18, United States Code. Those factors include (a) the nature and circumstances of the offense and the history and characteristics of the defendant; (b) the kinds of sentences available; (c) the advisory guideline range; (d) the need to avoid unwarranted sentencing disparities; (e) the need for restitution; and (f) the need for the sentence to reflect the following: the seriousness of the offense, promotion of respect for the law and just punishment for the offense, provision of adequate deterrence, protection of the public from future crimes and providing the defendant with needed educational or vocational training, medical care, or other correctional treatment. *See* 18 U.S.C. § 3553(a).

In this case a sentenced of 12 months and one day is sufficient, but not greater than necessary to achieve the goals of sentencing. This is based on Mr. Bondars' history and character, his nature and role in the offense, the flaws in the fraud guidelines, and the need to avoid unwarranted sentencing disparities,

I. A sentence no greater than 18 months is appropriate based on Mr. Bondars' history and character

Mr. Bondars is not a hardened cyber-criminal. As the submitted letters attest, he is a loving son and brother, and dedicated employee. Mr. Bondars' ex-girlfriend explained,

that even after they separated, she still knows Ruslans to be reliable, hard-working, supportive, and strong. *See* Def.'s Sentencing Ex. A, *Letter from Alina Pavlova.* Several of Mr. Bondar's colleagues advised the Court that Ruslans is kind and helpful, often staying late at work to help or complete a project. *See id.*, *Letters from Anastasia Dolgovechnaya; Genadijs Pugacovs; Olga Cipruse; Sergey Telshevsky.* In addition to these qualities, Ruslans' friend and colleague, Maksim Goncharov described Ruslans as "…passionate about technologies and challenging tasks and who always liked to share his knowledge to anyone interested." *Id.* Even Ruslans' subordinates at work offered letters to the Court explaining that as a boss, Ruslans is encouraging, kind, and generous. *See Letter from Marina Libermane-Onipko.*

Mr. Bondars is not only an incredible person at work, he also cares for his disabled sister. As several letter attested, Mr. Bondars is protective and attentive in this regard. *See id.* Mr. Bondars' girlfriend described Mr. Bondars as introspective, generous, and loving. She is living only a "half-life," in an agonizing wait for Ruslans to be her husband, and father to their children. *See id., Letter from Karina Valtere.*

One of the letters of support for Mr. Bondars described the way in which he matured and became a different person from 2006 to 2015. This is particularly relevant to sentencing in this case because almost all of the troubling conduct (particularly the 404(b) chat messages and contact with Martisevs) occurred during these earlier years. Mr. Bondars' subordinate, Nikolay Shulga first worked for Ruslans in 2006-2007. He then left the company and returned to work for Ruslans in 2015. Mr. Shulga offered very perceptive thoughts. He observed,

> Ruslan of 2006 was young ambitious person searching for his place in this life. That time Ruslan wanted to change a lot and everywhere. As a manager,

> he was quite impatient. Speaking with him one could easily note a solid bit of arrogance. His decision making approach was mostly in a flavor of what could be called "let's destroy and only then let's build from the ground"

He explained that when he returned to work for Ruslans after eight years, "Ruslan of 2015 surprised me a lot. In many aspects he was a different personality. He became patient with people, truly interested in opinion of subordinates. He communicated much softer with others. Impatience and arrogance completely disappeared. He turned into an experienced well skilled manager. His managerial skills evolved quite materially." Mr. Shulga actually commented on this change, he wrote that "In 2015, after working with Ruslan for several weeks, I put a direct question to him. I said I remember him different, I described the differences I saw. He replied, he really worked hard to change his nature and he still was continuing to evolve and work on himself." Mr. Shulga finally discussed the positive influence Ruslans has had on the young IT professionals in his community, stating that "The whole company is waiting for his return." *Id.*

II. Mr. Bondars nature and role in the offense was limited to administering a publicly available online automated website. It was a generic tool that comprised an optional small piece of malware.

Mr. Bondars' nature and role in the offense was significantly different from Shames, Huddleston, and Martisevs. Mr. Bondars did not develop *or sell* malware. *See* T.T. 580, *Testimony of Agent Kim* ("Q: Did you ever find any evidence of that? A: No, I did not."). Both Shames and Huddleston actually developed malware – a keylogger, and a Remote Access Tool (RAT) that included a keylogger, password downloader, webcam monitor, and file access. The purpose, and *only* purpose of their malware was to infiltrate a computer system and extract personal information. The Government eloquently summed up the nature of Shames and Huddleston's offenses—"Malware developers like

[Shames/Huddleston] are the root cause of computer hacking." *United States v. Zachary Shames*, 1:16CR289 – LO, *Gov. Position on Sentencing*, ECF No. 30 at 2; *United States v. Taylor Huddleston*, 1:17CR34-LO, ECF No. 40 at 12. The Government said "In the cybercrime world, malware developers are at the heart of the problem." *Shames*, ECF No. 30 at 9; *Huddleston*, ECF No. 40 at 13. Conversely, Mr. Bondars' role in the offense was limited to administering a publicly available online automated website. It was a generic tool that comprised an optional small piece of malware.

It would be disingenuous for the Government to allege that a malware developer or user *required* Scan4You for the success of his malware. The Court heard testimony from Shames, Belorossov, and Vartanyan who all indicated that their malware performed without Scan4You for a period of time, even for years. *See* T.T. 63; T.T. 137-38; T.T. 195, *Testimony of Agent Mark Ray* (stating he does not know whether every Citadel user used Scan4You); T.T. 221, *Testimony of Mark Vartanyan* (noting that the Citdel existed and operated prior to Scan4You); T.T. 257, *Testimony of Dimitri Belorossov* ("Q: … you don't actually need the Scan4you service for the toolkit itself to work, right? A: That's correct."). Furthermore, of the 29-50 files found on Target servers related to the data breach, only *five* of them were run through Scan4You. Thus, those other dozens of files (including the most potent ones) made it through Target's lists without the assistance of Scan4You. *See* T.T. 823, *Testimony of Heather Shannon.*

Computer hackers *need* malware to hack, and while possibly helpful, they do not *need* Scan4You to commit their crimes. *See* T.T. 137-38; T.T. 195; T.T. 221; T.T. 257; T.T. 63, *Testimony of Jim Cowardin*, ("Q: A malware developer doesn't have to use either of these two options [cypter or counter-antivirus]? A: No, they do not"). The

Government was correct when it said that "malware developers are the heart of the problem." And those who are the heart of the problem should be punished commensurate with that sentiment.

III. Table 2B1.1 provides little guidance on sentencing in this case.

The fraud guidelines are not particularly instructive in this case because this is not a situation in which Mr. Bondars stands before the Court alone, as part of an abstract computer conspiracy, in which the Court must conjure an academic formula in an effort to tether his situation to others across the nation.

Instead, in this case, the Court has had before it, four individuals who discussed their involvement in this conduct, with two of those individuals having been sentenced before this Court. Thus, Court has significantly broader, and more relevant information, upon which to base its sentence, and should not have to rely on theoretical calculations of loss and offense levels that is often required in more abstract situations. Therefore, a variance from the Guidelines is warrant to avoid disparities with others sentenced in this case before this Court.

IV. Table 2B1.1 is severely flawed.

The fraud loss table is fundamentally flawed as a matter of principle. Mr. Bondars' advisory guideline range calculated by the probation office is mainly driven by a single enhancement for the value amount under USSG § 2B1.1. This fraud loss guideline contains severe flaws. The guideline range offers no useful advice because it (1) is not based on empirical evidence or national experience, particularly with respect to the $500 per access device number; (2) uses the highly imperfect measure of "loss," to determine the seriousness of the offense; (3) has been widely discredited, and (4)

prescribes punishment that is grossly disproportional to the offense and far greater than necessary to promote the goals of sentencing in this case. Together these flaws produce a guideline that is manifestly unjust.

i. §2B1.1 is not rooted in empirical evidence generally

When Congress enacted the Sentencing Reform Act of 1984, it ordered the Commission to establish guidelines that "assure the meeting of the purposes of sentencing," 28 U.S.C. §991(b)(1)(A), and to use average sentences and incarceration time actually served in the pre-guidelines period as a "starting point." 28 U.S.C. § 994(m). The Commission was then directed to continually review and revise the guidelines in light of sentencing data, criminological research, and consultation with frontline actors in the criminal justice system. *See* 28 U.S.C. § 991(b)(1)(C), § 991(b)(2), § 994(o), § 995(13), (15), (16).

In *Rita v. United States*, 551 U.S. 338, 350 (2007), the Supreme Court discussed two reasons that it may be "fair to assume" that the guidelines "reflect a rough approximation of sentences that might achieve § 3553(a)'s objectives." First, the original Commission used an "empirical approach" which began "with an empirical examination of 10,000 presentence reports setting forth what judges had done in the past." Second, the Commission is able review and revise the guidelines based on judicial response through sentencing judgments, and consultation with other interest groups and experts. *Id*. at 348-50.

However, when the Commission established the guidelines in 1987, it "decided to abandon the touchstone of prior past practice" with respect to white collar offenses. Justice Stephen Breyer, *The Federal Sentencing Guidelines and the Key Compromises*

Upon Which They Rest, 17 Hofstra L. Rev. 1, 23 (1988).[5] The Commission prescribed at least a form of confinement for all but the least serious cases, and established a fraud guideline that required no less than 0-6 months and no more than 30-37 months for defendants in Criminal History Category I. *See* USSG § 2F1.1 (1987). The Commission explained that "the definite prospect of prison, though the term is short, will act as a significant deterrent to many of these crimes, particularly when compared with the status quo where probation, not prison, is the norm." USSG, ch. 1, intro., pt. 4(d) (1987).

This deterrence-based rationale was not supported by empirical evidence. Research on white-collar defendants shows no difference between the deterrent effect of probation and that of imprisonment. *See* David Weisburd et al., *Specific Deterrence in a Sample of Offenders Convicted of White Collar Crimes*, National Institute of Justice Report at 21-25 (1994) ("It has often been assumed by scholars and policy makers that white collar criminals will be particularly affected by imprisonment. Our findings provide evidence that this assumption is wrong, at least as regards reoffending among those convicted of white collar crimes in the federal courts.") [hereinafter *Specific Deterrence*].[6] Furthermore, "[T]here is no decisive evidence to support the conclusion that harsh sentences actually have a general and specific deterrent effect on potential white-collar offenders. In fact, when criminal sanctioning was found to have such an effect, it was accompanied by informal sanctions (such as social censure, shame, and loss of respect) which were equally important in producing the deterrent outcome." Zvi D.

---

[5] Available at http://scholarlycommons.law.hofstra.edu/cgi/viewcontent.cgi?article=1630&context=hlr, (last accessed July 20, 2018).

[6] Full report available at https://www.ncjrs.gov/pdffiles1/Digitization/151296NCJRS.pdf, (last accessed July 20, 2018).

Gabbay, *Exploring the Limits of the Restorative Justice Paradigm: Restorative Justice and White Collar Crime*, 8 Cardozo J. Conflict Resol. 421, 448-49 (2007)(emphasis added).

Exacerbating this injustice, prison sentences continued to increase for fraud offenses without any empirical support. In 1989, just two years after the Guidelines were enacted, three levels were added for a loss amount over $5 million. *See* USSG, App. C, Amend. 154 (Nov. 1, 1989). The official reason for the amendment was that the Commission sought to "increase the offense levels for offenses with larger losses to provide additional deterrence and better reflect the seriousness of the conduct." *Id*.

In 2001, offense levels were again increased for higher loss amounts pursuant to the Commission's Economic Crimes Package. *See* USSG, App. C, Amend. 617 (Nov. 1, 2001). The Commission explained that it was responding to "comments received from the Department of Justice, the Criminal Law Committee of the Judicial Conference, and others, that [the fraud guideline] under-punish[es] individuals involved in moderate and high loss amounts, relative to penalty levels for offenses of similar seriousness sentenced under other guidelines." *Id*. The Commission did not identify the "other guidelines" to which it referred, but it is obvious from the proceedings which discussed the amendment, that it referred to the drug guidelines. U.S. Sent'g Comm'n, *Symposium on Federal Sentencing Policy for Economic Crimes and New Technology Offenses* at 54-55 (2000).[7]

This alone establishes that the increase was flawed, for the drug guidelines were not based on empirical data or national experience. *See Gall*, 552 U.S. at 46, n.2;

[7] Available at http://www.ussc.gov/sites/default/files/pdf/research-and-publications/research-projects-and-surveys/economic-crimes/20001012-symposium/ePlenaryIII.pdf, *last visited on July 20, 2018.*

Kimbrough, 552 U.S. at 96. Moreover, basing white-collar guidelines on drug sentences means that the white-collar guidelines were not based on empirical data or national experience for white-collar crimes. When a guideline "do[es] not exemplify the Commission's exercise of its characteristic institutional role," because the Commission "did not take account of 'empirical data and national experience,'" the sentencing court is free to conclude that the guideline "yields a sentence 'greater than necessary' to achieve § 3553(a)'s purposes, even in a mine-run case." *Kimbrough*, 552 U.S. at 109-10.

ii. The Application Note assigning $500 per access device number lacks an empirical basis.

Not only does §2B1.1 lack an empirical basis generally, it's lack of empirical evidence is particularly glaring with respect to the $500 per access device provision. Application note (F)(i) to §2B1.1 demands that $500 be applied to every unauthorized access device number in a fraud case, and it is an entirely arbitrary amount, archaic in today's time.

When the Guidelines were originally promulgated in 1987, this application note prescribed a minimum of $100 per unauthorized access device. *See* 1987 USSG §2B1.1 Application Note 4.[8] The basis for this original $100 was unclear. The access device amount was then amended in 2000 in response to a 1998 directive from Congress. *See* Amend. No. 596 (Nov. 1, 2000), amending USSG §§ 2B1.1, 2F1.1. The directive instructed the commission to evaluate in part, "the extent to which the value of the loss caused by the offenses (as defined in the Federal sentencing guidelines) is an adequate

[8] Available at https://www.ussc.gov/sites/default/files/pdf/guidelines-manual/1987/manual-pdf/Chapter_2_A-C.pdf (last accessed Sept 10, 2018).

measure for establishing penalties under the Federal sentencing guidelines;" *See* Section 2 of the Wireless Telephone Protection Act, Pub. L. 105–172 ("WTPA"))

The Commission published a working group report setting forth its findings with respect to Congress' directive and the resulting amendments. USSC, *Cellular Telephone Cloning* (2000).[9] This working group report showed that the Treasury Department sought an increase to $1,000 per access device. In support of this request, the Treasury Department cited a 1999 study of credit card industry data that showed approximately $1,000 average fraud loss per card.

Instead of adopting the $1,000 per access device, however, Commission simply split the difference. It said:

> "Increasing the current minimum from a $100 to a $1,000 minimum value may be problematic in another way. For example, in cases where loss for some pairs is determined to be less than $1,000, using a $1,000 per card minimum for other pairs within the same case could be inappropriate. This problem would not likely occur if the current $100 minimum was retained. For those who argue that the $100 amount is too low for access devices, an amount somewhere in between $100 and $1,000 might be less problematic."

Id. at p. 27 (footnote omitted). Thus, not only was this change not based on empirical evidence at the time, any evidence it did have surround it, is drastically outdated.

The Treasury Department's data was from 1999. Presumably technology had not evolved in such a way that it was possible to cull troves of card numbers, as is possible today. Because of this, the average loss amount today is likely far lower – likely pennies, or even a fraction of a cent. In fact, the Government's own evidence in this case

[9] Available at http://www.ussc.gov/Research/Working_Group_Reports/Intellectual_Property_and_Tech/20000125_Cell_Phone_Cloning/cloning.PDF (last accessed Sept. 7, 2018).

illustrates this perfectly. All three individuals who had their information compromised by the limitless logger did not have a penny in loss. *See* T.T. 682, *Testimony of Michael Caple*; T.T. 691, *Testimony of Andrew Lee*; T.T. 691-7. It is almost routine today, to receive a notice from one's bank that a credit card number has been compromised, yet not suffer any financial loss. That is not to say losses don't occur. However, the average loss per access device number is likely far lower than it was in Treasury Department's 1999 data.

Even if the Treasury department's data were to reflect that average loss per card compromised, the data would still be off with respect to the guideline provision because it likely does not factor in its average all the access device numbers that may have been stolen, but never touched, or expired numbers, or access devices that are otherwise unusable. Yet, the guidelines require that the loss include these credit card numbers even if they are expired or otherwise unusable. See USSG §2B1.1, comment. (n.3(A)(ii)). It makes no sense to say intended, but impossible-to-obtain loss amounts provide an accurate reflection of offender culpability, particularly, when the offender, as is the case here, obtained *diminimus* amounts of money compared to a $20.5 billion intended loss. There is certainly no scenario in which Mr. Bondars would have ever envisioned himself a billionaire through Scan4You.

Judge Underhill said this best in *United States v. Corsey*, "Because the plan was farcical, the use of intended loss as a proxy for seriousness of the crime was wholly arbitrary: the seriousness of this conduct did not turn on the amount of intended loss any more than would the seriousness of a scheme to sell the Brooklyn Bridge turn on whether the sale price was set at three thousand dollars, three million dollars, or three billion

dollars. By relying unquestioningly on the amount of the intended loss, the District Court treated this pathetic crime as a multi-billion dollar fraud—that is, one of the most serious frauds in the history of the federal courts." 723 F.3d 366, 378-79, (2d Cir. 2013) (Underhill, D.J., concurring).

iii. "Loss" is a highly imperfect measure of the seriousness of the offense and overlaps with other enhancements

The amount of "loss" primarily determines the offense level for fraud offenders. However, loss is an extremely imperfect gauge as to the seriousness of the offense. *See United States v. Gupta*, 904 F.Supp.2d 349 (S.D.N.Y. Oct. 24, 2012) ("By making a Guidelines sentence turn, for all practical purposes, on this single factor, the Sentencing Commission effectively ignored the statutory requirement that federal sentencing take many factors into account, *see* 18 U.S.C. § 3553(a), and, by contrast, effectively guaranteed that many such sentences would be irrational on their face."); *United States v. Adelson,* 441 F. Supp. 2d 506, 509 (criticizing "the inordinate emphasis that the Sentencing Guidelines place in fraud on the amount of actual or intended financial loss" without any explanation of "why it is appropriate to accord such huge weight to [this] factor[ ]"). The amount of loss is "a relatively weak indicator of [ ] moral seriousness . . . or the need for deterrence." *See United States v. Emmenegger*, 329 F. Supp. 2d 416, 427-28 (S.D.N.Y. 2004).

"An amount of loss… does not tell us anything about why the defendant committed the offense or how much he personally benefited. These motive-based facts are important for issues of retribution, deterrence, and the need for incapacitation." David Debold & Matthew Benjamin, ''*Losing Ground''—In Search of a Remedy for the Overemphasis on Loss and Other Culpability Factors in the Sentencing Guidelines for*

Fraud and Theft, 160 U. Pa.L.Rev. PENNumbra 141, 152 (2011). A former staff attorney at the U.S. Sentencing Commission recently wrote, "[D]ecreasing the now-central role loss has in sentencing economic crimes is imperative…. Until then, courts and practitioners are well advised to look critically, and indeed skeptically, on the sentencing advice given by the Guidelines that are influenced by loss." Mark H. Allenbaugh, *"Drawn from Nowhere": A Review of the U.S. Sentencing Commission's White-Collar Sentencing Guidelines and Loss Data*, Federal Sentencing Reporter 26 (2013).

United States Sentencing Guideline §2B1.1 originally identified "loss" as a rough proxy for culpability because it reflected both "harm to the victim" and "gain to the defendant." *Losing Ground* at 150-51. In conspiracy cases where the measure is based on so tangential, this logic does not hold. *See Adelson*, 441 F. Supp. 2d at 510 (noting that the irrationality of the Guidelines in fraud cases are exacerbated for someone like the defendant, "who had no role in originating the conspiracy but only joined it in its latter stages… but will still be legally responsible under the guidelines for the full loss amount he could reasonably foresee.")(citing *United States v. Studley*, 47 F.3d 569, 574 (2d Cir. 1995).

In this case, using the loss amount is an even more absurd measure of the seriousness of the offense. The amount -- $20.5 Billion – represents the loss from an act of one user out of the 31,000 users of Scan4You. It represents five hash values (which *were* identified by Target's antivirus software) scanned through Scan4You out of millions of hashes scanned, and five hash values out of at least 29 hash values responsible for the data breach.

Furthermore, $20.5 Billion is an arbitrary amount assigned to the alleged number of access device numbers seized in this singular act. There is no information about the authenticity of these device numbers, whether they were used, or intended to be used, whether they were old, defective, or duplicates.

More importantly, this figure in no way represents even close to the comparatively miniscule amount of money Mr. Bondars' received. Mr. Bondars' service charged five cents to scan a file and a $15 monthly subscription. His gain had absolutely no connection to his customer's later activities. Mr. Bondars did not stand to benefit whether his customers caused $5 in loss or $500,000 in loss. Thus, evaluating Mr. Bondars' culpability on an arbitrarily assigned amount caused by a random user of his service defies logic and does not conform to the original principals upon which USSG §2B1.1 was founded.

C. The fraud guidelines have been widely discredited and prescribe punishment that is grossly disproportional to the offense and far greater than necessary to promote the goals of sentencing in this case.

Judges across the country have noted the severe flaws in the fraud Guidelines. These Guidelines are not "heartlands" contemplated by *Rita*, 551 U.S. at 351. In fiscal year 2016, sentences within the guideline range were imposed in only 42.7% of all fraud cases – less than half of all cases. *See* U.S. Sent'g Comm'n, 2016 *Sourcebook of Federal Sentencing Statistics*, tbl.27.[10] "[I]t is difficult for a sentencing judge to place much stock in a guidelines range that does not provide realistic guidance." *Parris*, 573 F. Supp. at

[10] Available at https://www.ussc.gov/sites/default/files/pdf/research-and-publications/annual-reports-and-sourcebooks/2016/Table27.pdf, *last visited July 20, 2018.*

751; (*see also United States v. Watt*, 707 F. Supp. 2d 149 (D. Mass. 2010) (noting that the "Guidelines were of no help."). Judge Frederick Block notably derided the severity of loss-driven sentences as "a black stain on common sense." *Parris*, 573 F. Supp. 2d at 751.

Other judges have recognized this as well. *See United States v. Corsey,* 723 F.3d at 378 ("The widespread perception that the loss guideline is broken leaves district judges without meaningful guidance in high-loss cases; that void can only be filled through the common law, which requires that we reach the substantive reasonableness of these sentences."); *United States v. Faulkenberry*, 759 F. Supp. 2d 915, 928 (S.D. Ohio 2010), aff'd, 461 Fed. App'x 496 (6th Cir. 2012) ("As has become common among district courts sentencing white-collar offenders in financial fraud cases, the Court finds that the loss calculation substantially overstates the gravity of the offense here and declines to impose a within-Guidelines sentence."); *Gupta*, 904 F. Supp. 2d at 351 (Guidelines "reflect an ever more draconian approach to white collar crime, unsupported by empirical data.").

The increases in the fraud guideline have led to the absurd result that first-time, nonviolent fraud offenders are subject to ranges higher than those applicable to the most violent offenders. Judge Frederick Block stated, "[t]he staggering increases in sentence ranges driven by the amount of loss combined with largely duplicative sentencing enhancements have escalated advisory guidelines sentences for high-loss frauds beyond those once reserved for violent criminals." *Parris*, 573 F. Supp. 2d at 751.

E. A Guidelines sentence would create a severe unwarranted disparities among other fraud cases.

The Court should avoid unwarranted disparities among defendants other fraud

cases. As explained above, the Court has before it, fourt other individuals in this case who committed worse offenses – they are more culpable – and were sentenced to six months, 48 months, 54 months, and 60 months. Additionally, the individual known as reFUD.me in this case, who offered a similar scanner and his own malware, was sentenced to two years in the United Kingdom.

CONCLUSION

For the above reasons, Mr. Bondars respectfully requests that he be sentenced to 18 months incarceration. Mr. Bondars further requests that the Court recommend FCI Fort Dix, and that he be permitted to serve a portion of his sentence in Latvia pursuant to the International Prisoner Transfer Program, so that he may be closer to his family.

Respectfully Submitted,
RUSLANS BONDARS
By Counsel
HARRIS CARMICHAEL & ELLIS, PLLC
/s/
Jessica N. Carmichael, Esq. VSB# 78339
Yancey Ellis, Esq. VSB# 70970
Counsel for Defendant,
108 N. Alfred Street, 1st Floor
Alexandria, Virginia 22314
(703) 684-7908
(703) 649-6360 (fax)
jcarmichael@harriscarmichael.com
yellis@harriscarmichael.com

CERTIFICATE OF SERVICE

I hereby certify that on this 14th day of September, 2018, I filed the foregoing pleading through the ECF system, which shall then send an electronic copy of this pleading to all parties in this action.

/s/
Jessica N. Carmichael